CLAIMS

1. A digital signal processing method, comprising:

configuring a portion of an array of independently reconfigurable processing elements for performing a block cipher routine; and

executing the block cipher routine on data blocks received at the configured portion of the array of processing elements.

2. The method of claim 1, wherein configuring a portion of the array of reconfigurable processing elements includes activating the portion with an activation signal.

3. The method of claim 2, wherein configuring a portion of the array of reconfigurable processing elements further includes loading a plurality of subkeys into the active processing elements.

4. The method of claim 2, wherein configuring a portion of the array includes loading a context instruction into one or more active processing elements, wherein the context instruction configures logical elements within a processing element for performing one of a plurality of subfunctions of the block cipher routine.

5. The method of claim 3, wherein loading a plurality of subkeys occurs at a first cycle of the block cipher routine.

6. The method of claim 4, wherein loading the context instruction is repeated at subsequent cycles.

7. The method of claim 4, wherein executing the block cipher routine includes executing one of the plurality of subfunctions according to the context instruction.

8. The method of claim 3, wherein configuring a portion of the array includes loading, at each of a plurality of subsequent cycles, a context instruction into one or more active processing elements, wherein each context instruction configures logical elements within a processing element for performing one of a plurality of subfunctions of the block cipher routine.

9. The method of claim 8, wherein executing the block cipher routine includes executing the plurality of subfunctions on the input data blocks according to the context instruction and using corresponding subkeys.

10. The method of claim 1, wherein the array of reconfigurable processing elements includes an M-row by N-column number of processing elements.

11. The method of claim 1, wherein the block cipher routine is the KASUMI block cipher.

12. The method of claim 3, wherein the plurality of subkeys include the KL, KO, and KI subkeys of the KASUMI block cipher.

13. The method of claim 4, wherein the plurality of subfunctions include the FL and FO subfunctions of the KASUMI block cipher.

14. The method of claim 13, wherein the plurality of subfunctions further includes the FI subfunction within the FO subfunction.

15. The method of claim 13, wherein the plurality of subfunctions further includes one or more logic operations.

16. The method of claim 12, wherein the configured portion of the array includes at least four processing elements.

17. The method of claim 13, wherein the context instructions are loaded into two active processing elements.

18. The method of claim 11, wherein the data blocks received at the configured portion of the array are each 64 bits in length.

19. The method of claim 1, wherein the data blocks are non-encrypted, and wherein the method further comprises outputting encrypted data from the configured portion of the array of processing elements, wherein the encrypted data is encrypted according to the block cipher routine.

20. The method of claim 1, wherein the data blocks are encrypted, and wherein the method further comprises outputting decrypted data from the configured portion of the array of processing elements, wherein the decrypted data is decrypted according to the block cipher routine.

21. A digital signal processing method, comprising:

receiving an input data block at an array of independently reconfigurable processing elements;

configuring a portion of the array of processing elements for performing a block cipher routine; and

executing the block cipher routine on the input data block; and

outputting an output data block from the array, the output data block being transformed from the input data block by the block cipher routine.

22. The method of claim 21, wherein the input data block is unencrypted data, the block cipher routine is an encryption routine, and the output data block is encrypted data.

23. The method of claim 21, wherein the input data block is encrypted data, the block cipher routine is a decryption routine, and the output data block is decrypted data.

24. The method of claim 21, further comprising generating, with the configured portion of the array, a cipher key with which the block cipher routine is executed.

25. The method of claim 21, wherein configuring the portion of the array includes configuring one or more processing elements for performing a plurality of subfunctions of the block cipher routine.

26. The method of claim 25, wherein the block cipher routine is the KASUMI block cipher.

27. The method of claim 24, wherein the cipher key includes the KL, KO and KI subkeys of the KASUMI block cipher.

28. The method of claim 26, wherein the plurality of subfunctions includes the FL and FO subfunctions of the KASUMI block cipher.

29. The method of claim 28, wherein the FO subfunction further includes the FI subfunction of the KASUMI block cipher.

30. The method of claim 21, wherein the array includes an M-row by N-column number of reconfigurable processing elements.

31. A digital signal processing apparatus, comprising:

a context memory for storing one or more context instructions for performing a block cipher routine; and

an array of independently reconfigurable processing elements, each of which is responsive to a context instruction for being configured to execute a portion of the block cipher routine.

32. The apparatus of claim 31, further comprising a data bus, connected to the array of processing elements, for providing input block data on which the block cipher routine is executed.

33. The apparatus of claim 32, further comprising a direct memory access controller for controlling the transfer of the input block data, and for controlling the output of the result of the block cipher routine executed on the input block data.

34. The apparatus of claim 31, wherein the array of processing elements includes an M-row by N-column number of processing elements.

35. The apparatus of claim 34, wherein the context memory includes a row context memory for instructing each of the M rows of processing elements.

36. The apparatus of claim 34, wherein the context memory includes a column context memory for instructing each of the N columns of processing elements.

37. The apparatus of claim 31, wherein the block cipher routine is the KASUMI block cipher.

38. The apparatus of claim 37, wherein at least one context instruction is adapted to configure one or more processing elements for generating one or more subkeys of the KASUMI block cipher.

39. The apparatus of claim 37, wherein at least one context instruction is adapted to configure one or more processing elements for executing one or more subfunctions of the KASUMI block cipher.

40. The apparatus of claim 39, wherein the one or more subfunctions include the FL and FO subfunctions.

41. The apparatus of claim 31, wherein each processing element includes one or more functional units that, when activated, perform a selectable logic function.